Using Hebbian Network for Cipher

Amera Istiqlal Badran **Nidal Hussein Al-Asadi**
amera_istiqlal@uomosul.edu.iq
College of Computer Sciences and Mathematics
University of Mosul, Iraq

Received on: 06/10/2008 **Accepted on: 04/12/2008**

ABSTRACT

This research contains two parts, in the first part, a ciphering system is built using the classical Hebbian network to protect data against many expected threats during the transfer of the data. In the second part, deciphering has been built by using the Hebbian neural network.

The time has been calculate for both cipher and decipher. In the ciphering process, a Hebbian network has been developed through a qualitative primary weight which has large value. Then, an equation has been applied to minimize the weight matrix. Here, The idea of Stream Ciphering has been used so as to feed the network entries at the ciphering stage. The work has been applied by using (Visual Basic) language, issue (6.0) with the Object Oriented Programming (OOP) on a computer of the (P III, 600MHz) type.

Keywords: ciphering system, Hebbian network, Object Oriented Programming (OOP), Visual Basic) language.

استخدام شبكة (Hebbian) في التشفير

عامرة استقلال بدران **نضال حسين الاسدي**
كلية علوم الحاسبات والرياضيات/ جامعة الموصل

تاريخ استلام البحث: 06/١٠/٢٠٠٨ **تاريخ قبول البحث: 04/١٢/٢٠٠٨**

الملخص

يحوي هذا البحث على جزئين:

في الجزء الأول تم بناء خوارزمية للتشفير عن طريق استخدام شبكة (Hebbian) التقليدية لحماية البيانات ضد الكثير من التهديدات المتوقعة التي تتعرض لها أثناء نقل البيانات.أما الجزء الثاني فقد تم بناء خوارزمية لفك الشفرة عن طريق استخدام الشبكة العصبية(Hebbian).

وفي كلا الجزئين تم حساب الوقت المستغرق أي التشفير وفك الشفرة لمعرفة كم من الوقت تستغرق. وفي عملية التشفير تم تطوير شبكة (Hebbian) وذلك من خلال وزن أولي نوعي الذي يكون حجمه كبير، إذ تم تطبيق معادلة عليه مما أدى إلى تصغير مصفوفة الوزن . وقد تم استخدام فكرة التشفير الانسيابي لغرض تغذية مداخل الشبكة في مرحلة التشفير. وضع هذا العمل قيد التطبيق باستخدام لغة (Visual Basic) الإصدار (6.0) مع أسلوب البرمجة الشيئية وطبق العمل على حاسبة من نوع (PIII,600MHz).

الكلمات المفتاحية: نظام تشفير، شبكة Hebbian، أسلوب البرمجة الشيئية، لغة (Visual Basic).

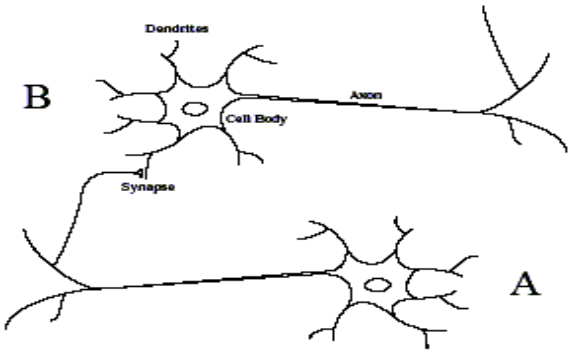
1. المقدمة

من الضروري التوجه إلى الشبكات العصبية الاصطناعية التي تعد من التطبيقات الحديثة في مجال الذكاء الاصطناعي إذ اعتمدت على أسس بيولوجية في محاولة محاكاة السلوك البشري[4] .

تم في هذا البحث اخذ فكرة التشفير الانسيابي بدون استخدام القواعد المحددة لطريقة التشفير، ونتيجة لهذا العمل تم تغذية شبكة (Hebbian) بإدخالات الملف وتم إجراء عملية التشفير باستخدام هذه الشبكة ومن ثم تمت عملية فك الشفرة الناتجة من عملية التشفير أيضاً باستخدام شبكة (Hebbian).

2. شبكة Hebbian:

لقد تم اكتشاف شبكة (Hebbian) من قبل العالم دونالد هيب (Donald Hebb)عام 1949. حيث قدم العالم (Hebb) أول قاعدة لتعليم الشبكة العصبية اطلق عليها (Hebbian learning Rule) اعتمدت كقاعدة أساسية لتطوير خوارزميات التعليم[1][7]. وان الهدف من هذه الشبكة هو إعادة تعديل مصفوفة الوزن التي تمثل مصفوفة الارتباط بين العقد. أي انه في حالة تدريب شبكة (Hebbian) فان الأوزان بين عقد الشبكة سيتم تعديلها وفقاً لعلاقات التمثيل بين العقد. وقد تم اعتماد شبكة(Hebbian) بصورة أساسية في إعادة تعديل مصفوفة الوزن فاذا كانت احتمالية العقدة (A) تثير العقدة (B) بصورة عالية نسبياً، فان قوة الترابط بين العقدتين (A) و(B) سوف تزداد، وتسمى هذه الحالة بالتعلم من الذاكرة (Learning from Memory) وذلك لان الشبكة سوف تستخدم المعلومات المستنبطة من الأحداث السابقة لغرض تعديل الوزن بين العقد المترابطة كما في الشكل(1)[10] .

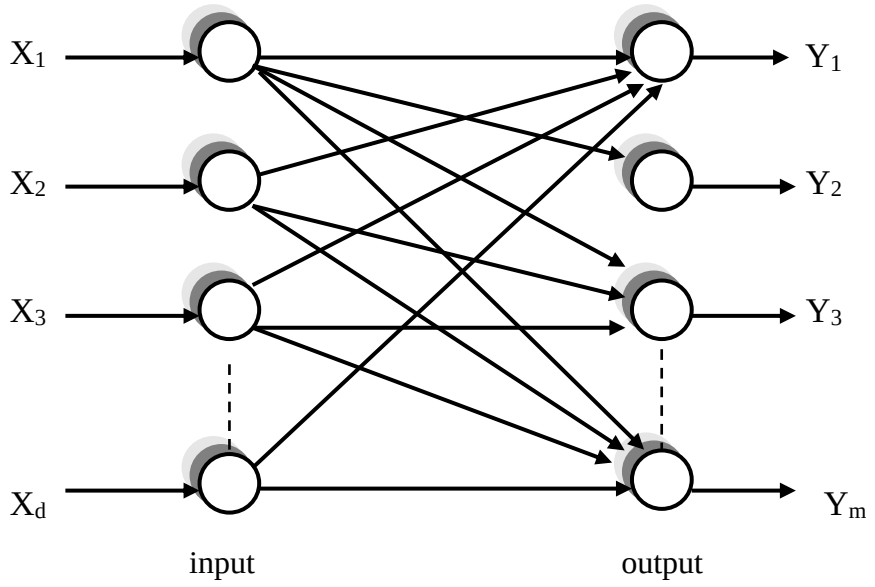


الشكل (1):يوضح تأثير عقدة على عقدة أخرى

إن نموذج التعلم لشبكة (Hebbian) يمكن أن يقع تحت أسلوبين وهما: التدريب بمعلم، والتدريب بدون معلم [9]. وقد تم استخدام شبكة (Hebbian) بدون معلم في هذا البحث، وتمتاز شبكة (Hebbian)من نوع بدون معلم بأنها تتكون من طبقة واحدة، أما اتجاه سير العمل فيها يكون من نوع السير إلى الأمام. وتمتاز هذه الشبكة بعدم احتواء جسم الخلية على دالة التحفيز، بينما يحدث التحديث على الوزن[6] .

معمارية شبكة (Hebbian):

يبين الشكل(2) الآتي بصورة عامة معمارية شبكة (Hebbian) التي تتكون من طبقة واحدة ويتم فيه توضيح الإدخالات والاخراجات.



الشكل(2):مخطط يوضح معمارية شبكة (Hebbian)

لأجل الحصول على قيم الاخراج يمكن متابعة المعادلة الآتية:-

$$y_j(n) = \sum_{i=1}^{d} W_{ji}(n) * X_i(n) \rightarrow j = 1,2,.....,m \qquad \ldots(1)$$

- لأجل تعديل مصفوفة الوزن فيمكن متابعة المعادلة الآتية:-

$$\Delta W_{IJ}(n) = \eta(n) y_j(n) \left[X_i(n) - \sum_{k=1}^{j} W_{ki}(n) y_k(n) \right] \qquad \ldots(2)$$

for $i = 1,2,.....,d$ and $j = 1,2,.....,m$

حيث ان:-

X_i = تمثل قيمة الادخال i .

y_j = تمثل قيمة الاخراج j .

W_{ij} = تمثل قيمة مصفوفة الوزن ij .

ΔW= التعديل في مصفوفة الوزن.

η = معامل التعلم $= \frac{1}{n^{\alpha}}$ $\frac{1}{2} < \alpha \leq 1$

m = عدد قيم الاخراج.

d = عدد قيم الادخال.

n = عدد الدورات.

خوارزمية شبكة Hebbian:-

يمكن التوصل الى خوارزمية شبكة (Hebbian) من خلال الخطوات الاتية:[6]

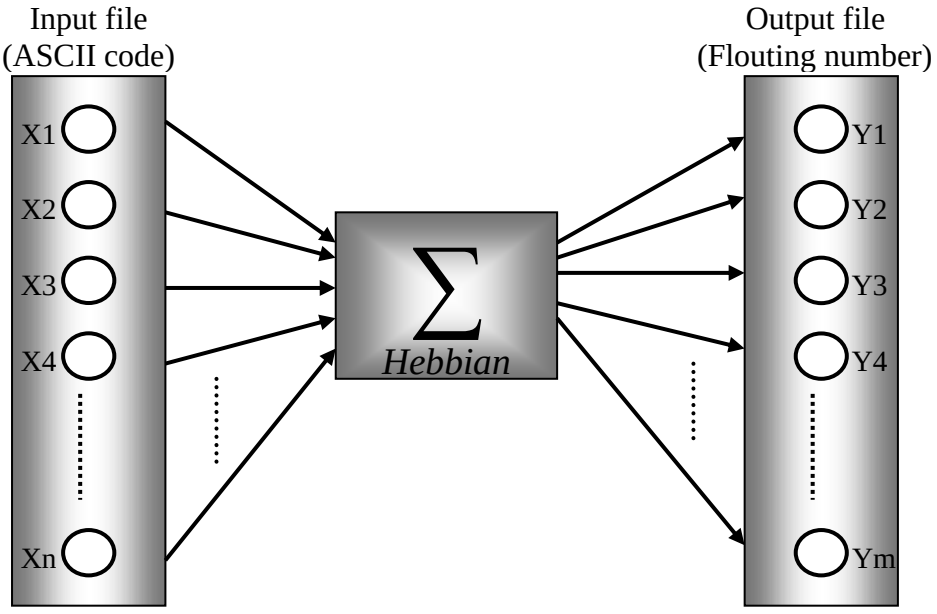
1. تهيئة مصفوفة الوزن بقيم عشوائية عند (n=1). وتخصيص قيمة موجبة صغيرة لـ(η).
2. حساب المعادلتان (1)ثم (2).
3. زيادة (n) بقيمة واحدة والذهاب إلى الخطوة الثانية، الاستمرار بالدوران إلى حد الوصول إلى القيمة الثابتة.

لقد تم توضيح خطوات العمل في خوارزميتين الاتيتين:[3]

الخوارزمية الأولى تتضمن خطوات عملية تشفير النص المدخل إلى شبكة (Hebbian). الخوارزمية الثانية تتضمن خطوات فك تشفير النص باستخدام شبكة (Hebbian).وبعد تطبيق خوارزمية التشفير وفك الشفرة يتم حساب الوقت المستغرق لكل حالةً.ولقد تم استخدام شبكة (Hebbian) في التشفير وذلك لان هذه الشبكة تمتاز بأنها خطية أي ان لها أسلوب خطي في عملية حساب الاخراجات[10], علماً ان هناك فوائد اخرى اضافية في التشفير اللاخطي ولكن تم استخدام هذه الطريقة لانها لا تحتوي على طبقة خفية مما يؤدي إلى زيادة سرعة تدريب الشبكة نسبياً بالاضافة الى عدم احتوائها على دالة التحفيز, اضافة إلى سهولة استخدام معادلات حساب الاخراجات ومعادلات تعديل الوزن[6].

3. خوارزمية التشفير:

- تبدأ عملية التشفير باستخدام شبكة (Hebbian) باعتماد الخوارزمية الآتية (الشكل(3))[3]:-

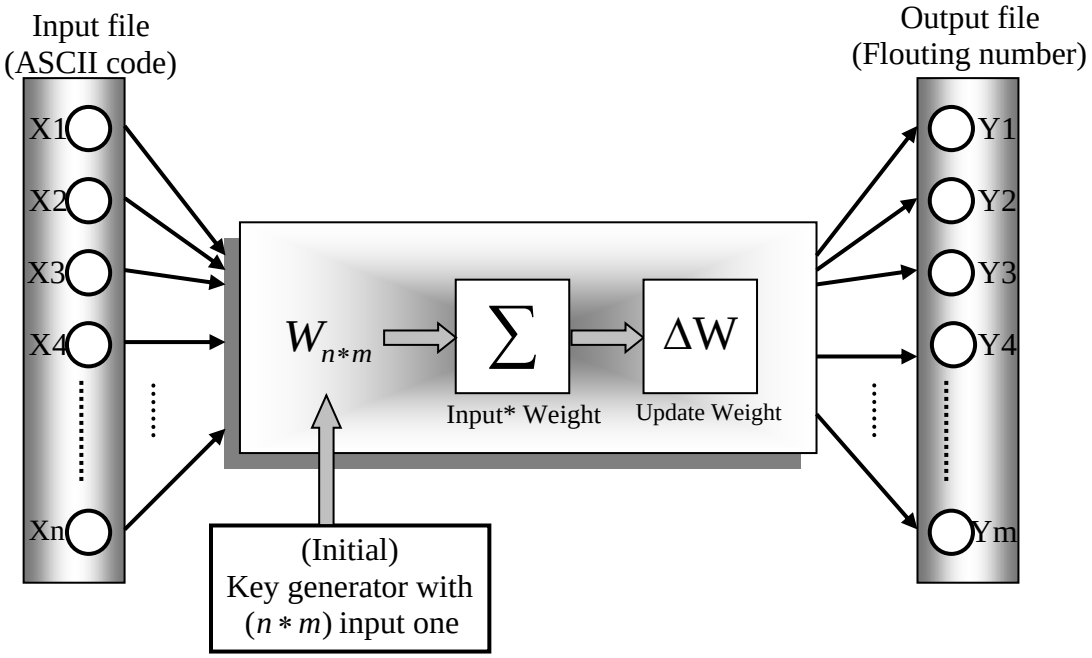


الشكل(3):مخطط عام لعملية التشفير باستخدام شبكة(Hebbian)

1- فتح الملف المراد تشفيره .

2- تهيئة حجم مصفوفة الوزن بحجم الملف.

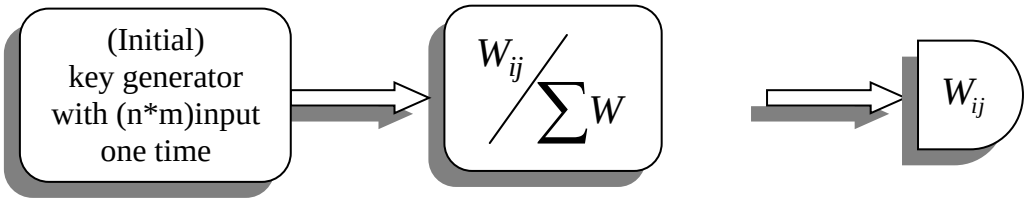
3- توليد مفاتيح عشوائية وإحلالها إلى مصفوفة الوزن (الشكل (4)).



الشكل (4):مخطط تفصيلي لعملية التشفير باستخدام شبكة**(Hebbian)**

4- أجراء عملية تسوية(Normalization) لمصفوفة الوزن لتجنب حصول حالة تجاوز للقيم وذلك بالاعتماد على معادلة التبسيط الآتية:

$$W_{ij} = W_{ij} \Big/ \sum W \qquad ...(3)$$



الشكل(5):مخطط تفصيلي يوضح عملية تسوية(Normalization) لمصفوفة الوزن

إن إجراء عملية التعديل على مصفوفة الوزن وذلك من اجل تصغير قيم مصفوفة الوزن التي تم تكوينها بطريقة عشوائية كما في الشكل أعلاه (الشكل(5)).

5- تحديد إدخالات الشبكة من خلال القيم المقابلة لكل حرف بشفرة اسكي في الملف.

6- البدء عند (n=1).

7- تهيئة قيمة صغيرة لـ(η).

8- حساب اخراجات الشبكة من خلال اعتماد معادلة رقم (1).

9- تعديل مصفوفة الوزن من خلال اعتماد معادلة رقم(2).

10- زيادة قيمة (n) بقيمة واحدة.

11- الرجوع إلى الخطوة (7).

بعد الانتهاء من عملية التدريب لـ(n) لخطوات عدة، يتم الحصول على قيم الاخراجات التي تمثل القيم المشفرة المقابلة لكل حرف مدخل. وتمثل عدد عقد الاخراجات بعدد عقد الإدخالات أي ان (d=m).

تعتبر مصفوفة الوزن الناتجة من الدورة الأخيرة لـ(n) هي المفتاح الذي سوف يتم استخدامها في عملية فك الشفرة[8]. ومن الجدير بالذكر انه قد تم الاستفادة من فكرة التشفير الانسيابي في عملية تغذية شبكة (Hebbian) بالإدخالات[3].

4. خوارزمية فك الشفرة:

تبدأ عملية فك الشفرة باستخدام شبكة (Hebbian) من خلال اعتماد الخوارزمية الآتية (الشكل(6))[3]:-

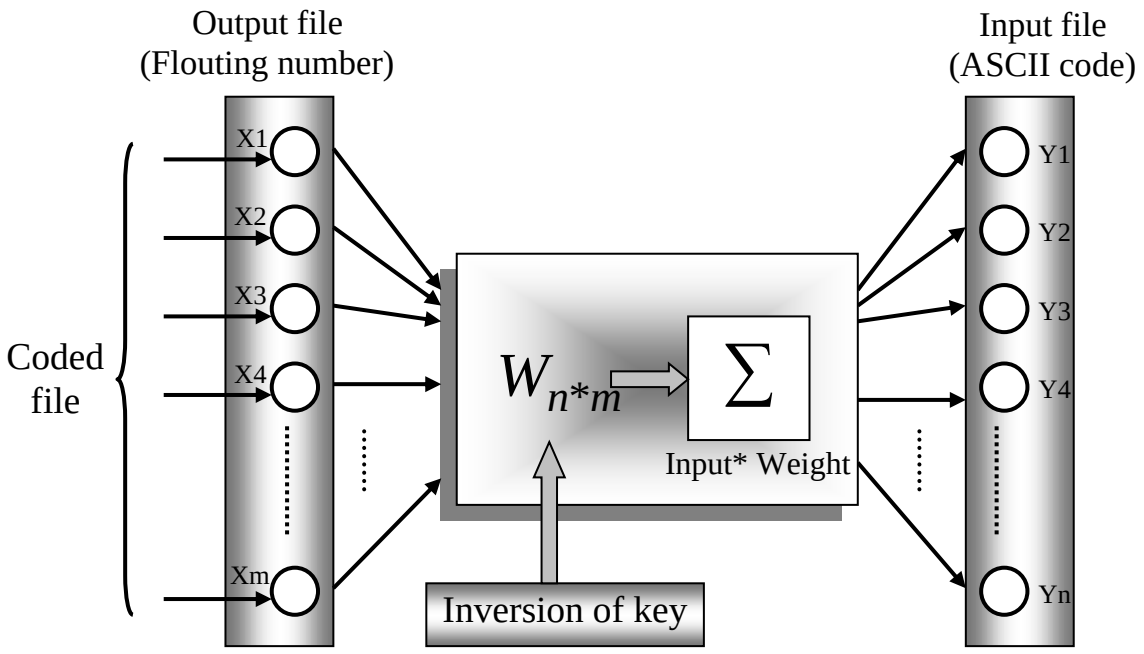
1- فتح الملف المشفر وتهيئته كإدخالات .

2- تهيئة مصفوفة الوزن التي تمثل مصفوفة المفاتيح بقيم مصفوفة الوزن الناتجة من عملية التشفير.

3- حساب معكوس المصفوفة لمصفوفة الوزن، (أي اخذ آخر مصفوفة تم الحصول عليها من عملية التحديث على الوزن التي تم إجراءها بتطبيق معادلة رقم(2) ومن ثم حساب معكوس المصفوفة.

4- حساب اخراجات الشبكة من خلال اعتماد معادلة رقم (1).

5- تمثلت اخراجات الشبكة القيم الصريحة للنص الأصلي بشفرة اسكي.



الشكل(6)

مخطط تفصيلي لعملية فك الشفرة باستخدام شبكة(Hebbian)

ولقد تم محاولة تهجين شبكة (Hebbian) مع الخوارزمية الجينية لعملية التشفير وفك الشفرة، إذ كانت الخوارزمية الناتجة تسمى بالخوارزمية الهجينة ولكن عند إجراء العمل تبين أن العملية تكاد أن تكون من الناحية العملية مستحيلة وذلك لان الخوارزمية الجينية تعتمد على تشفير قياسي أما الشبكة العصبية فهي تعتمد على التشفير غير القياسي وبهذا أصبح وجود تناقض ما بين الطريقتين بسبب هذا الاختلاف. وذلك لصعوبة تحديد معادلة مدى اللياقه[3].

5. خوارزمية حساب الوقت:

إن عملية حساب الوقت المستغرق في عملية التشفير أو فك الشفرة يتم حسابه باعتماد الخوارزمية الآتية:[3]

1- قراءة قيمة الوقت قبل عملية التشفير أو فك الشفرة بـ(دقيقة/ثانية).

2- إجراء عملية التشفير أو فك الشفرة.

3- قراءة قيمة الوقت بعد الانتهاء من عملية التشفير أو فك الشفرة بـ(دقيقة/ثانية).

4- حساب الوقت لإجراء عملية التشفير أو فك الشفرة(الوقت المستغرق) باعتماد المعادلة الآتية:

الوقت المستغرق=الوقت بعد العملية(تشفير أو فك الشفرة)– الوقت قبل العملية(تشفير أو فك الشفرة).

ان سبب استخدام خوارزمية لحساب الوقت لغرض التأكد من ان الوقت المستغرق لا يزيد عن الحد المعقول ولذلك تم قياس الوقت المستغرق وفيما بعد الشكل(8) يوضح قياس الوقت المستغرق للتشفير وفك الشفرة وكيف ان الوقت المستغرق في فك الشفرة اطول من التشفير وذلك بسب عملية الحساب لمعكوس المصفوفة.

6. التطبيق العملي للخوارزمية

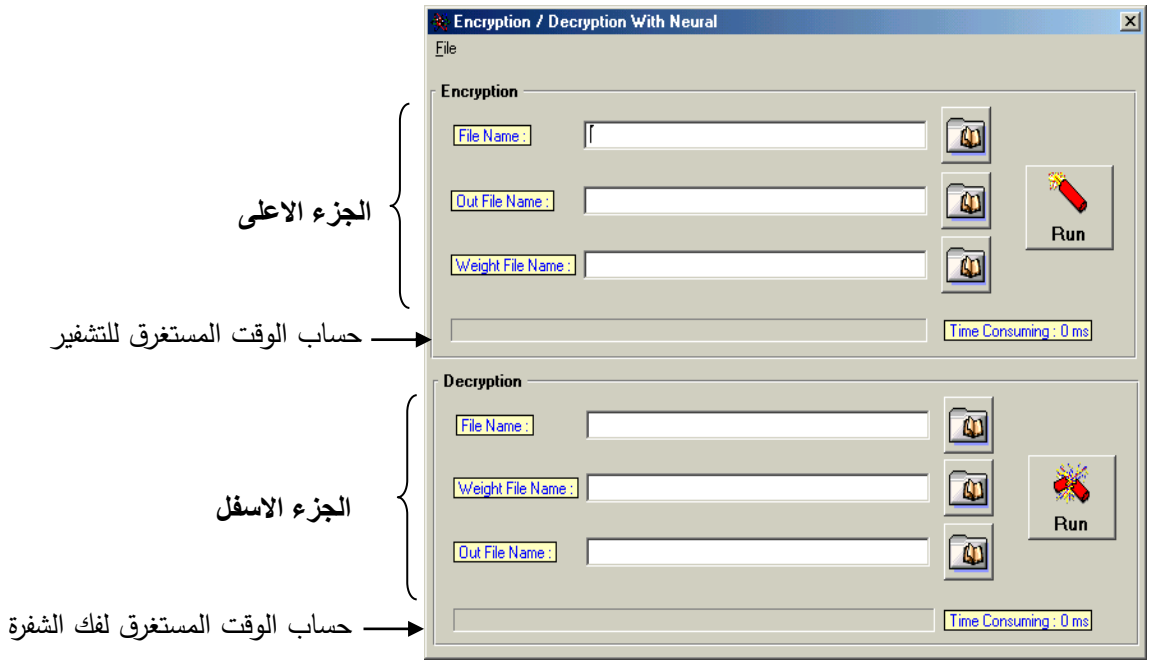
في هذا الجزء من البحث سوف نتطرق إلى عملية تنفيذ البرنامج الذي تم تنفيذه باستخدام لغةVisual Basic 6.0[2][5] ويمكن تتبع خطوات التنفيذ عن طريق المراحل الآتية:

7. الجزء التنفيذي للبرنامج

عند تنفيذ البرنامج سوف تظهر الشاشة الآتية كما في الشكل (7) والتي تحوي علىجزئين:

الاول: الجزء الاعلى خاص بالتشفير مع حساب الوقت المستغرق للتشفير .

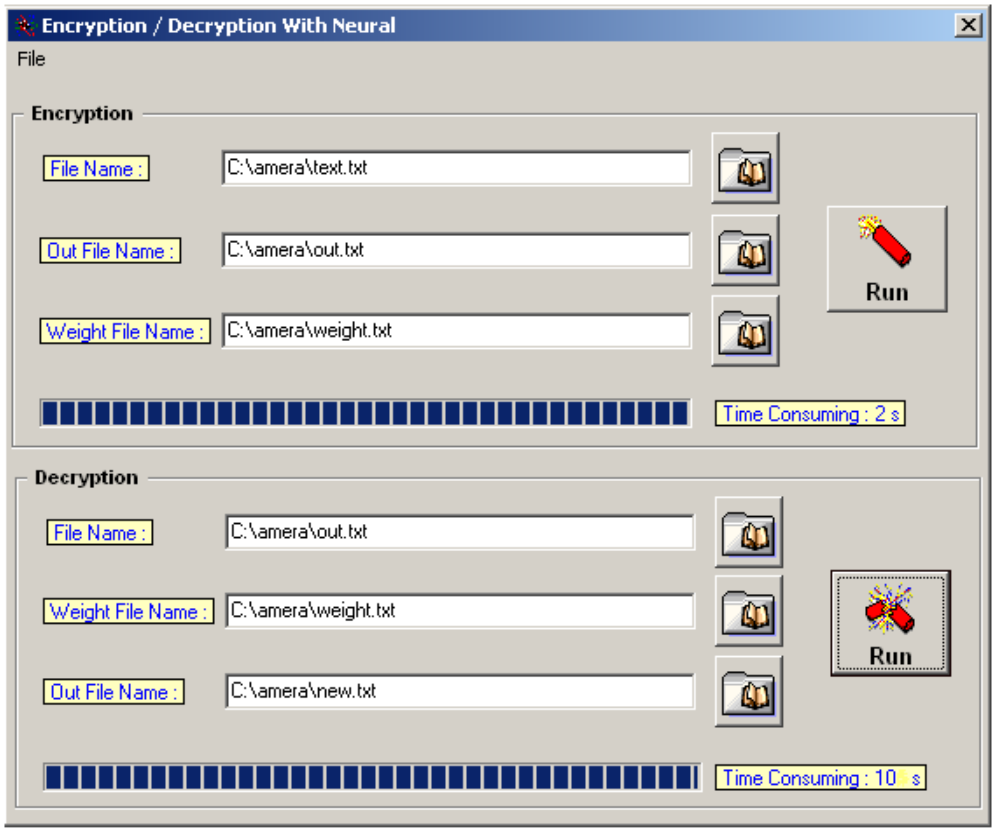
الثاني: الجزء الاسفل خاص بفك الشفرة مع حساب الوقت المستغرق لفك الشفرة.



الشكل (7) نافذة بداية تنفيذ البرنامج

اذا كان النص ذات حجم صغير جداً فأن الوقت المستغرق في عملية التشفير وفك الشفرة يقاس بأجزاء الثانية لذلك فان الوقت المستغرق في التشفير وفك الشفرة يساوي اقل من الثانية الواحدة.

مثال توضيحي للوقت المستغرق في التشفير وفك الشفرة, حيث أن الوقت المستغرق في التشفير 2s والوقت المستغرق في فك الشفرة 10s , نلاحظ بان الوقت في فك الشفرة اطول من وقت التشفير كما في الشكل(8).



الشكل (8)

نافذة حساب الوقت

8. نتائج تنفيذ البرنامج:

❖ **مثال :**

- محتويات الملف (Test.txt) قبل عملية التشفير:

Microsoft Corporation

- محتويات الملف (Output.txt) بعد عملية التشفير والتي تمثل القيم المقابلة لكل حرف:

229472	**270831**	**350196**	**224732**	**316244**	**366492**	**232854**
277980	**229456**	**295496**	**171597**	**280570**	**277579**	**276161**
304861	**294848**	**317306**	**298337**	**347712**	**332726**	**282559**

محتويات الملف (New.txt) بعد عملية فك الشفرة:

Microsoft Corporation

يجب ملاحظة من الجدول اعلاه ان هناك زيادة في طول الرقم المشفر الناتج المقابل لرمز النص. حيث يحتاج الى تحليل مفصل لغرض ايجاد اقل نسبة من طول النص المشفر الى غير المشفر علماً ان العملية تتم بواسطة تغيير دقة الحسابات في الشبكة العصبية الاصطناعية ولم يتم اخذها بنظر الاعتبار في هذا البحث لان التركيز في امكانية عمل الشبكات العصبية الاصطناعية في التشفير وخاصة شبكة (Hebbian).

الاستنتاجات

إن عملية التشفير باستخدام الشبكة العصبية(Hebbian) تتضمن نوعاً من السرية العالية بسبب كبر المفتاح نسبياً وذلك لكونه يمثل مصفوفة ثنائية ذات أبعاد بحجم النص. وان عملية فك الشفرة تتطلب وجود (مصفوفة الوزن) التي تمثل مفتاح (فك الشفرة). بالإضافة إلى أن حجم الملف الناتج من عملية التشفير يكون اكبر من حجم الملف الأصلي لان طبيعة البيانات الناتجة تكون أرقاماً حقيقية. ومن المهم أن نعرف إن الوقت المستغرق في عملية التشفير يكون (بالاعتماد على عدد الدورات)، ومتناسب بشكل طردي مع حجم النص بالإضافة إلى أن الوقت المستغرق في عملية فك الشفرة يكون كبيرا وذلك بسبب عملية الحساب لمعكوس المصفوفة. ولقد تم التأكد من صحة النتائج في عملية فك الشفرة بنسبة (100%).

التوصيات:

1. التأكد المفصل من ان النظام الشفري أمين من خلال تطبيق الاختبارات الخاصة بالعشوائية على النص المشفر.
2. استخدام شبكة تتكون أكثر من طبقة للمقارنة بين الوقت المستغرق في عملية التشفير وشبكة (Hebbian) أحادية الطبقة.
3. استخدام فكرة التشفير الكتلي في عملية تغذية مداخل الشبكة في حالة كون الملف المشفر كبيراً.
4. القيام على توفير سرية عالية على (مصفوفة الوزن) الناتجة من عملية التشفير (مصفوفة المفاتيح).
5. تطبيق فكرة التهجين في الشبكات العصبية الاصطناعية وخاصة مع شبكة (Hebbian) للحصول للحصول على وزن قياسي أمثل. وممكن أن نستغني عن معادلة الوزن في شبكة(Hebbian) باستخدام الخوارزمية الجينية.
6. إدخال عملية كبس لمصفوفة الوزن باستخدام أسلوب الكبس بالشبكات العصبية (شبكة Backprobagation) لغرض تقليص حجم المصفوفة.

المصادر

[1] العبيدي، محمود خليل ابراهيم (2000): "الشبكات العصبية الاصطناعية"، مجلة أبحاث الحاسوب، مدرس علم الحاسوب، الجامعة التكنلوجية، بغداد.

[2] الناظر، سائد محمود (1997): "كتاب المبرمج Visual basic 5.0"، دار شعاع للنشر والعلوم، سورية حلب, الطبعة الأولى.

[3] بدران, عامرة استقلال (2003):"استخدام شبكة (Hebbian) في التشفير"بحث ماجستير, كلية علوم الحاسبات والرياضيات, جامعة الموصل.

[4] سليمان، أنعام محمد (2002): "التداخل الشبكي الجيني (GA-Hf) لحل المسائل من نوع Np-problem (TSMP)"، بحث ماجستير، كلية علوم الحاسبات والرياضيات، جامعة الموصل.

[5] هالفرسون، مايكل (1999): " Visual basic 6.0 خطوة خطوة"، الدار العربية للعلوم، لبنان.

[6] Haykin, S. [1999]: "Neural Network: A comprehensive Foundation", Second edition, prentice Hall, London. ,CH2.

[7] Patterson, Dan W. (1996): “Artificial neural networks, theory and application”, Prentice Hall.

[8] WWW.comp.glam.ac.uk/digimag.

[9] WWW.csse.monash.edu.au/~app/L01.pdf.

[10] WWW.cs.hmc.edu/courses/ch07-pres.pdf.